Control Administrative Privileges

Administrative privileges on a computer system allow access to resources that are unavailable to most users and permit the execution of actions that would otherwise be restricted. When such privileges are administered improperly, granted widely, and not closely audited, attackers are able to exploit them and move effortlessly through a network.

Gaining administrative privileges is commonly achieved through a technique known as privilege escalation. Privilege escalation is defined as the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain access to resources that are unavailable to normal users. Poorly managed administrative privileges make executing this technique much easier.

Who is at Risk?

In “Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques,” Microsoft® identifies several factors that indicate that an organization is at risk for privilege escalation attacks in their Windows® environment[1]. These risk factors include:

- Privileged accounts (e.g., Domain Administrators) regularly log on to user workstations.
- Privileged users conduct non-administrative tasks (e.g., surfing the web, reading email).
- Normal (non-administrator) users are members of the local workstation Administrators group.
- The default local Administrator accounts on workstations and servers have identical passwords.
- Application and/or service accounts are granted domain administrative or system privileges.

Recommendations

Below are recommendations for controlling administrative privileges on your network.

Do Not Allow Local Accounts to Access the Network

Local, non-service accounts generally do not require remote logon privileges in a Windows domain setting to perform their required tasks. Remove the network and remote interactive logon privileges from these accounts, especially administrator accounts. Denying local administrators remote access forces them to administer machines physically at the console. If physical administration is not possible, restrict remote logon to a few privileged users and only from well-secured workstations.

These changes can be implemented via Group Policy or local security policy. Add members of the local Administrators group to two user rights: “Deny access to this computer from the network” and “Deny log on through Remote Desktop Services.”

Restrict Systems that Privileged Accounts Can Access

Users may inadvertently expose their privileged account credentials when they perform general administration tasks. Limit these highly privileged accounts so they can only log on to secure systems, thereby reducing the likelihood of exposing privileged credentials to higher risk computers.

Remove Standard Users from the Local Administrators Group

Do not grant standard user accounts membership in the local Administrators group. This simple step creates an additional barrier that an adversary must overcome in order to obtain local administrative access.

Ensure Administrative Accounts Do Not Have Email Accounts or Internet Access

Privileged accounts should not be used to perform general tasks such as accessing emails and browsing the Internet. Additionally, on servers, disable/remove browsing and e-mail capability altogether if not necessary for the server applications to function. Email and Internet browsing activities are inherently dangerous because they may involve processing information that is potentially malicious. If accounts with administrative privileges are used to perform these activities, a potential compromise can lead to immediate attacker control of those rights.

Follow the Principle of Least Privilege

Members in privileged groups are high value targets for attackers. Reduce the number of members in these groups and only give users the permissions they need to do their jobs. Very few users should have domain admin credentials, and domain admin logons should be used only for activities that require that privilege level.

Use Multi-Factor Authentication

In order for users to be granted access to network resources, make them prove that they are who they say they are. The user can be authenticated by what he has (e.g. an ID card or token), what he knows (e.g. a password or PIN), or what he is (e.g. biometric data). For all privileged accounts, use a robust authentication process that requires at least two of these factors.

Manage Passwords Effectively

Text passwords are inherently weak and can be cracked or compromised given enough time and effort. If multi-factor authentication is not possible, passwords for administrative accounts should be complex and contain a combination of letters, numbers, and special characters. Additionally, they should be of a sufficient length (generally for Windows systems, greater than 14 characters). Consider using longer passphrases instead of typical passwords. Require regular password changes for all administrative and other privileged accounts, and ensure the passwords are different from other accounts. Finally, if passwords are stored for emergency access, keep these in a protected off-network location, preferably in a safe.

Additional Information

- Best Practices for Securing Active Directory
  http://www.microsoft.com/en-us/download/details.aspx?id=38785

- Enforcing No Internet or Email from Privileged Accounts
  http://www.nsa.gov/ia/_files/factsheets/Final_49635NonInternetsheet91.pdf

- Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques
  http://www.microsoft.com/en-us/download/details.aspx?id=36036

- Reducing the Effectiveness of Pass-the-Hash
  http://www.nsa.gov/ia/_files/app/Reducing_the_Effectiveness_of_Pass-the-Hash.pdf

- Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines
  http://www.sans.org/critical-security-controls/

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**

Disclaimer of Endorsement: Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

[1] Microsoft® and Windows® are registered trademarks of Microsoft Corp.